IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Jong-Uk CHOI et al.	Examiner: Bayat, B.
Application No.: 10/034,485	Group Art Unit: 3621
Filed: December 28, 2001	
Attorney Docket No.: 01122_1000 Client Docket No.: 200601-0001/US	

For: METHOD FOR SECURING DIGITAL INFORMATION AND SYSTEM THEREFOR

APPEAL BRIEF

Honorable Commissioner for Patents
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal dated September 27, 2007.

I.   REAL PARTY IN INTEREST

MarkAny Inc. is the real party in interest, as evidenced by the assignment set forth at Reel 012427, Frame 0533.

II.   RELATED APPEALS AND INTERFERENCES

Appellants bring to the attention of the Honorable Board the filing of an Appeal Brief on July 12, 2007, in U.S. Patent App. Serial No. 10/375,181, entitled "System For Protecting and

Managing Digital Contents," which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the present appeal. As of the filing of the present appeal, no decision is believed to have been rendered by the Board in response to the Appeal Brief filed on July 12, 2007, in U.S. Patent App. Serial No. 10/375,181.

III. STATUS OF THE CLAIMS

Claims 1-19 have been canceled, and claims 20-40 remain pending. Pending claims 20-23, 27-38, and 40 have been withdrawn from consideration as being drawn to a non-elected invention. This appeal is therefore taken from the final rejection of elected claims 24-26 and 39, as set forth in the final Office Action dated April 27, 2007, and the Advisory Action dated September 18, 2007.

IV. STATUS OF AMENDMENTS

All amendments have been entered. No amendments were filed subsequent to the final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention addresses problems associated with security of transmissions of information over a network.

Independent claim 24 provides for the following:

24.   A method for providing security (see, e.g., page 4, lines 26-35), the method comprising:

creating a unique user key (see, e.g., page 10, line 32; and FIG. 3) using system information of a user terminal (see, e.g., element 14 in FIGs. 1 and 2; and page 10, lines 30-32); and

transmitting digital information and user information including the unique user key to a server system via a network (see, e.g., element 10 in FIGs. 1 and 2; page 5, lines 30-31; page 10, lines 32-37; and page 11, lines 10-14),

wherein the unique user key is transmitted by a user application tool installed in the user terminal for authentication (see, e.g., element 214 in FIG. 2; page 10, lines 31-33; and page 11, lines 3-5 and 10-14).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 24-26 and 39 are anticipated under 35 U.S.C. § 102(e) by *Fransdonk* (U.S. Pub. No. 2006/0210084).

VII. ARGUMENT

A. CLAIMS 24-26 AND 39 ARE NOT ANTICIPATED BY *FRANSDONK* BECAUSE *FRANSDONK* FAILS TO DISCLOSE ALL OF THE ELEMENTS RECITED IN THE CLAIMS.

As noted in MPEP §2131, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." (Quoting *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).) As will be demonstrated below, *Fransdonk* clearly does not meet each and every limitation recited in independent claim 24.

Independent claim 24 recites a method for providing security comprising creating a unique user key using system information of a user terminal, and transmitting digital information and user information including the unique user key to a server system via a network, wherein the unique user key is transmitted by a user application tool installed in the user terminal for authentication. *Fransdonk* does not disclose, either expressly or inherently, each and every element recited in independent claim 24. *Fransdonk* fails to disclose the **transmitting of digital information and user information including a unique user key, which is created using system information of a user terminal, to a server system, where the unique user key is transmitted by a user application tool installed in the user terminal**.

In rejecting claim 24 based on *Fransdonk*, the Examiner in the final Office Action dated April 27, 2007, merely listed paragraphs [0105], [0126], [0146], [0183], [0202], and [0210]-[0221], and did not provide any discussion of the relevance of these paragraphs with respect to the various elements recited in claim 24. Additionally, the Examiner did not elaborate on the grounds of rejection in the Advisory Action dated September 18, 2007, but rather merely indicated that the Appellants' traversal was not persuasive without any explanation as to why this conclusion was reached. Thus, at the outset, Appellants submit that the Examiner has failed to satisfy the burden set forth in 35 U.S.C. §132(a), which prescribes that "[w]henever, on examination, any claim for a patent is rejected, or any objection or requirement made, the Director shall notify the applicant thereof, stating the reasons for such rejection, or objection or requirement, together with such information and references as may be useful in judging of the propriety of continuing the prosecution of his application." The final Office Action and the Advisory Action do not provide any indication as to how the Examiner is interpreting the

information described in the cited paragraphs in *Fransdonk*, and an interpretation that reads on the claim elements is not self-evident or appropriate, as will be clear from the discussion below.

Fransdonk describes a method and system to securely store and distribute content keys. FIG. 1 illustrates, at a high-level, the processing of content as it is communicated from a content provider 16 to a content distributor 20 in a distribution process 12, and then from the content distributor 20 to a content destination 22 in a delivery process 14. *Fransdonk* describes the use of various types of keys, such as product (or content) keys, public keys, private keys, storage keys, secret (group) keys, and unique keys. For example, *Fransdonk* describes in paragraph [0047] that clear content 24 is encrypted at the content provider 16 utilizing, for example, a symmetric product key (or content key) to generate encrypted content 26. The encrypted content 26 (or cipher text) is then communicated from the content provider 16, via the network 18, to the content distributor 20. In one embodiment, the conditional access agent 28 decrypts the encrypted content 26 to regenerate the clear content 24 within a secure environment, and watermarks the clear content for distribution to a specific content destination 22. In an alternative embodiment, the conditional access agent 28 at the content distributor 20 may re-encrypted the content with a public key of a copy-protected device at the content destination 22.

The paragraphs of *Fransdonk* that were listed by the Examiner provide additional details regarding the method and system, and the cited paragraphs are summarized below.

Paragraph [0105] sets forth a MerchantUser table that "represents the users (operators) of content providers 16," which is generally described as being utilized by the conditional access server 36 (see paragraph [0098]). Paragraph [0105] indicates that the users (operators) of content provider 16 possess a secure token to access the conditional access server 36. The MerchantUser table is described as being "used to verify the identity of the content providers 16 when he or she

logs on to the system." The MerchantUser table notes that the serial number of a secure device is the unique key.

Paragraph [0126] notes that the conditional access agent 28 performs a gateway function after a subscriber is granted access to the content, including the sending of a request to local content server 40 to release the content, decrypting the content with one key, and then re-encrypting the content with a different key (e.g. a unique user key). Paragraph [0146] provides an exemplary operational scenario involving the conditional access agent 28, with reference to FIG. 5, including the selection of access criteria (e.g. that the serial number is not on the Certificate Revocation List as noted in Paragraphs [0150] and [0152]) and retrieving secure device information (as noted in paragraph [0155]).

Paragraph [0183], listed by the Examiner, indicates that an advantage of using distributed conditional access agents 28 to represent the interests of the service providers 16 (rather than providing direct access between subscribers and service providers) is that personal re-encryption of content by the conditional access agents 28 using unique user keys requires that an unauthorized distributor must redistribute the entire content, and not just the relevant keys.

Paragraph [0202] describes, in connection with the flowcharts shown in FIGs. 6A and 6B, the processing of a content request received from a content destination 22. Paragraph [0202] indicates that if the request passes the verification process, the conditional access agent 28 then establishes a secure session with the conditional access client 48, and generates a unique user key (U_k). The unique user key (U_k) is then encrypted with a public key of either a copy-protected device associated with the secure device 46, or the secure device 46 itself, and communicated to the conditional access client 48 using the secure session.

And paragraphs [0210]-[0217] describe, in connection with the flowchart of FIG. 7, a method of delivering content from a content provider 16 to a consumer via at least one content distributor 20. Paragraph [0210] again notes that the conditional access agent 28 generates a unique user key (U_k). The method also includes watermarking the content, re-encrypting the watermarked content with the unique user key, encrypting the unique user key, and encrypting the product key, and then sending the encrypted items to the consumer at the content destination 22, where they are decrypted for use. Furthermore, paragraphs [0218]-[0221] describe, in connection with the FIGS. 8A and 8B, the use of random, time-varying session keys, and the use of a unique user key (U_k) therewith using the conditional access agent 28.

Appellants submit that these paragraphs of *Fransdonk* that were listed by the Examiner in rejecting claim 24 do not anticipate claim 24, for the reasons discussed below.

Regarding the discussion in paragraph [0105], the MerchantUser table is a table utilized by the conditional access server 36, which acts as a content security access service provider (ASP) for merchants in the distribution process 12. (See, e.g. paragraphs [0068] and [0098], and the title in between paragraphs [0080] and [0081].) The MerchantUser table is described as being used to "verify the identity of the content providers 16 when he or she logs on to the system," and indicating that the Serial Field in the MerchantUser table is a unique key.

Appellants note that *Fransdonk* does not specify how the MerchantUser table is created, nor does it specifically describe how the information in the MerchantUser table is transmitted or manner in which it is used to verify the identity of the content providers. In fact, *Fransdonk* does not again mention logging on to the system. *Fransdonk* merely indicates that the MerchantUser table exists and is utilized by the conditional access server 36 to verify the identity of content providers when he or she logs on to the system. Thus, paragraph [0105] of *Fransdonk* does not

7

disclose **transmitting of digital information and user information including a unique user key, which is created using system information of a user terminal, to a server system, where the unique user key is transmitted by a user application tool installed in the user terminal.** *Fransdonk* does not describe the transmitting of any such information, for example, how information is transmitted and what element does the transmitting. *Fransdonk* also does not describe the creation of the MerchantUser table, or the process of logging in to the system other than briefly referring thereto in paragraph [0105]. Thus, Appellants submit that the discussion in paragraph [0105] of *Fransdonk* does not anticipate the subject matter recited in independent claim 24.

Fransdonk describes a conditional access agent 28 that "provides at least two functions namely (1) a verification function that includes verification of content destination (e.g., subscriber) requests for secure content against access criteria defined by a content provider 16, and (2) a gateway function including decryption, watermarking and re-encryption of secure content, depending on content security settings." (Paragraph [0122].) Regarding the verification function of the conditional agent 28, the conditional access agent 28 retrieves various information from a number of sources, such as secure device servers 44 located at commerce service providers 42 to verify information regarding the secure device (see paragraphs [0070] and [0127]-[0130]) and conditional access server 36 to query subscriptions, access criteria, and keys (see paragraphs [0132]-[0133]). (See also, FIG. 5, 6A, and 6B and the corresponding descriptions thereof.) Regarding the contact between the conditional access agent 28 and the conditional access client 48, which acts as a go-between between the secure device 46 of the subscriber and the conditional access agent 28, *Fransdonk* describes the conditional access agent 28 as interfacing with the conditional access client 48 "to send a payment request, receive a transaction

(signed payment request) and to pass any result messages (such as service denial based on insufficient debit/credit, regional blackout, etc)." (Paragraph [0134].) However, this description of the verification process in *Fransdonk* does not describe creating a unique user key using system information of a secure device 46, where the unique user key is transmitted by a user application tool installed in the secure device 46 for authentication, in the manner recited in claim 24.

Regarding the gateway function of the conditional access agent 28, *Fransdonk* describes the use of unique user keys (U_k), which are related to the distribution process 14, as they are used in the distribution of content from the conditional access agent 28 to the conditional access client 48. (See, e.g., paragraphs [0202] and [0210]-[0221] listed by the Examiner.) After passing the verification process, then the conditional access agent 28 generates a unique user key (U_k), and uses the unique user key to re-encrypt content that is then sent to a consumer at a content destination 22 for decryption. (See, e.g., paragraphs [0202], [0210], [0212], and [0213].) However, *Fransdonk* does not indicate that the "unique user key (U_k)" generated by the conditional access agent 28 is at any time **transmitted by a user application tool installed in the user terminal for authentication.** Assuming, solely for the sake of argument, that the unique user key (U_k) generated by the conditional access agent 28 is created using system information of secure device 46, the unique user key (U_k) is not described as being transmitted by a user application tool installed in the secure device 46, but rather is described as being generated by the conditional access agent 28 and sent to the conditional access agent 48 (see, e.g., paragraphs [0202], [0210]-[0213], [0221], and [0222]). *Fransdonk* does not describe the secure device 46 as including a user application tool installed therein that transmits the unique user key (U_k) at any stage.

Furthermore, *Fransdonk* does not specifically indicate that the "unique user key (U$_k$)" generated by the conditional access agent 28 is created using system information of a user terminal, but merely that it is created after the verification process. Furthermore, even if the Examiner is assuming that the "unique user key (U$_k$)" is the same feature as the "unique key" mentioned with regard to the MerchantUser table, which Appellants submit is not clear from the discussion in *Fransdonk*, the discussion in paragraphs [0202]-[0221] make clear that the unique user key (U$_k$) is sent from the conditional access agent 28 to the conditional access agent 48, and does not describe the unique user key (U$_k$) as being transmitted by a user application tool installed in the secure device 46.

Thus, Appellants respectfully submit that *Fransdonk* fails to disclose **transmitting of digital information and user information including a unique user key, which is created using system information of a user terminal, to a server system, where the unique user key is transmitted by a user application tool installed in the user terminal**, in the manner recited in claim 24 of the present application. Accordingly, Appellants traverse the anticipation rejection of independent claim 24, as the cited reference does not disclose, either expressly or inherently, each and every element recited in independent claim 24.

Furthermore, with respect to the anticipation rejection of claims 25, 26, and 39, which depend from independent claim 24, Appellants respectfully submit that claims 25, 26, and 39 are also not anticipated by *Fransdonk* for the reasons discussed above with respect to claim 24.
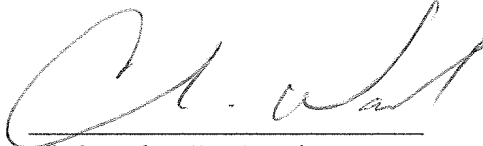
Therefore, the Honorable Board is respectfully requested to reverse the rejection of claims 24-26 and 39 under 35 U.S.C. § 102.

VIII. CONCLUSION AND PRAYER FOR RELIEF

For the foregoing reasons, Appellants request the Honorable Board to reverse each of the

Examiner's rejections.

Respectfully Submitted,
DITTHAVONG MORI & STEINER, P.C.

_11/27/2007_
Date

Christopher D. Ward
Attorney for Appellant(s)
Reg. No. 41367

918 Prince Street
Alexandria, VA 22314
Tel. 703-519-9952
Fax. 703-519-9958

IX.   <u>CLAIMS APPENDIX</u>

24. A method for providing security, the method comprising:

creating a unique user key using system information of a user terminal; and

transmitting digital information and user information including the unique user key to a server system via a network, wherein the unique user key is transmitted by a user application tool installed in the user terminal for authentication.

25. The method according to claim 39, wherein the rule includes one or more of authority of storage, authority of print, authority of allowable time for use, or authority of transfer of the data.

26. The method according to claim 24, wherein the system information includes at least one of unique CPU (Central Processing Unit) information, RAM (Random Access Memory) information, HDD (Hard Disk Drive) information, or serial number information of the user terminal.

39. The method according to claim 24, further comprising:

encrypting data and the user information including the unique user key transmitted from the user terminal;

storing the encrypted user information and the encrypted data in the server system;

establishing a rule corresponding to the user information and the data;

encrypting the rule and a decryption key for decrypting the digital information using the unique user key;

combining the encrypted data, the encrypted rule and the encrypted decryption key into combined information;

storing the combined information;

performing a user authentication process by comparing the unique user key stored in the server with the unique user key subsequently transmitted from the user application tool of the user terminal for authentication;

transmitting the combined information from the server system to the user application tool via the network after completing the user authentication process, when the user terminal requests a download of the data; and

determining, with the user application tool, whether the data should be decrypted by determining whether the key used for encrypting the decryption key matches the unique user key created by the user application tool.

X.   <u>EVIDENCE APPENDIX</u>

Appellants are unaware of any evidence that is required to be submitted in the present Evidence Appendix.

XI.   **RELATED PROCEEDINGS APPENDIX**

Appellants are unaware of any related proceedings that are required to be submitted in the present Related Proceedings Appendix.